Remarks

In the Office Action dated May 5, 2005, the Examiner rejected claims 1-33 under 35 U.S.C. § 102 as being anticipated by the U.S. Patent to Belissent 6,789,203.

By this Amendment, Applicants' Attorney has amended claim 19 to make it clearer that each of the independent claims now require that packet flow statistics are received and processed to generate one or more signals representing data packet flow anomalies and wherein the signal(s) is responded to by tracking attributes related to the anomalies back to at least one source or origin of the attack.

Clearly, this feature is neither taught, disclosed nor discussed by the U.S. Patent to Belissent taken either alone or in combination with any of the other references of record.

The U.S. Patent to Belissent is primarily concerned with preventing a denial of service attack without notifying the attacker. The invention of Belissent is an IP throttler for defending against a denial of service attack and recording all connecting IP addresses by allowing its server to detect attackers as soon as the volume of connection requests coming from a particular IP address is higher than would otherwise be expected. A firewall 206 is included in or coupled to a server computer 202 which monitors all incoming connection requests. The firewall 206 includes a throttler unit that is used to identify and prevent any denial of service attacks. The throttler unit includes a connection request monitor arranged to monitor the number of connection requests received by a particular requesting client based on the requesting client's IP address. A processor unit is configured to count the number of connection requests for a particular requestor based on the associated IP address per unit of time.

Belissent fails to disclose the generation of one or more signals or alert message representing anomalies based on processed packet flow statistics which signal(s) is responded to by tracking or tracing attributes related to the anomalies to a source or origin of the attacks.

Contrary to the Examiner's assertion, "tracking" of the present invention is not equivalent to "identifying" a denial service attack. The present invention relates to a method and system for detecting and tracking one or more denial of service attacks over a computer network as noted in the Title of the application, the Field of the Invention and Summary of the Invention. As noted on page 17, line 25 through page 18, line 14, the controller can apply one of several approaches to trace or track the attack back to its source or origin in order to uncover or form the path of the attack from its source or origin. An exemplary attack path is shown at 100 in Figure 7. Also, as identified at page 18, lines 15 and 16, only after "detection" and "tracing" occurs does "blocking" occur.

In summary, Belissent simply does not describe "tracing" or "tracking" back to the source or origin of an attack as only described and claimed in the present application.

Consequently, in view of the above and in the absence of better art, Applicants' Attorney respectfully submits the application is in condition for allowance which allowance is respectfully requested.

Respectfully submitted,

GERALD R. MALAN, ET AL.

By__________________
David R. Syrowik
Reg. No. 27,956
Attorney for Applicant

Date: June 17, 2005

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351